NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 23 (03/06/2024 – 09/06/2024)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Chiến dịch tấn công APT:** Chiến dịch tấn công mạng nhằm vào Đông Nam Á.

- **Cảnh báo:** TikTok khắc phục lỗ hổng zero-day sau chiến dịch chiếm dụng tài khoản người dùng.

2. Điểm yếu, lỗ hổng

- TOP **10** lỗ hổng đáng chú ý trong tuần.

3. Số liệu, thống kê

- **Tấn công DRDoS**

- **Tấn công Web**

- **Botnet ảnh hưởng tới người dùng Việt Nam**

- **Tấn công lừa đảo người dùng Việt Nam: 388** trường hợp lừa đảo do người dùng Internet Việt Nam thông báo.

4. Tài liệu lưu trữ

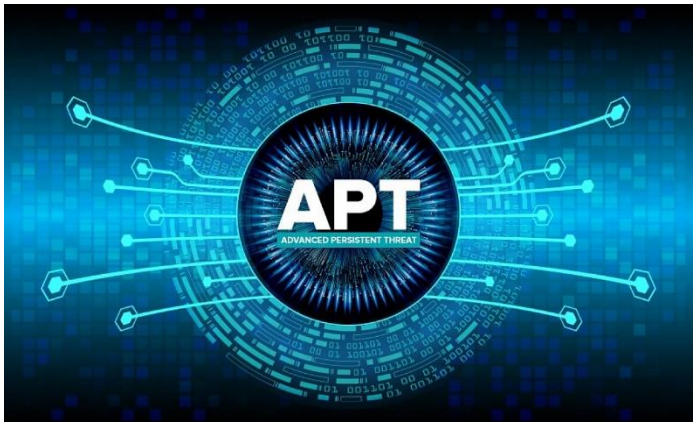
Chuyên mục **Cảnh báo tuần** tại địa chỉ:

https://khonggianmang.vn

NCSC VN
National Cyber Security Center

Tin tức An toàn thông tin

"Chiến dịch tấn công APT: Chiến dịch tấn công mạng nhằm vào Đông Nam Á"



Một tổ chức chính phủ giấu tên tại Đông Nam Á đã trở thành mục tiêu của chiến dịch tấn công mạng kéo dài và phức tạp, do **nhóm gián điệp mạng Crimson Palace** thực hiện.

Mục tiêu chính của chiến dịch là duy trì kết nối với mạng lưới của tổ chức này để thu thập thông tin có lợi cho Trung Quốc. Chiến dịch bao gồm xâm nhập hệ thống IT quan trọng, theo dõi người dùng, thu thập thông tin kỹ thuật và quân sự quan trọng, và phát tán mã độc để kết nối tới máy chủ C&C.

Nhóm tấn công Crimson Palace được chia thành ba cụm xâm nhập diễn ra vào các thời điểm khác nhau:

- **Cluster Alpha** (Từ tháng 03/2023 đến tháng 08/2023): Có điểm tương đồng với các nhóm tấn công như: BackdoorDiplomacy, REF5961, Worok, và TA428.
- **Cluster Bravo** (Tháng 03/2023): Có điểm tương đồng với nhóm APT Unfading Sea Haze.
- **Cluster Charlier** (Từ tháng 03/2023 đến tháng 04/2024): Có điểm tương đồng với nhóm Earth Longzhi, là một nhóm con của APT41.

Đáng chú ý, cuộc tấn công này sử dụng các mã độc chưa từng được ghi nhận trước đây như PocoProxy và phiên bản cập nhật của EAGERBEE, cùng với các mã độc khác như NUPAKAGE, PowHeartBeat, RUDEBIRD, DOWNTOWN (PhantomNet) và EtherealGh0st (còn gọi là CCoreDoor). Các đặc trưng nổi bật khác của chiến dịch bao gồm:

- **DLL Side-Loading**: Sử dụng kỹ thuật DLL side-loading rộng rãi để tránh bị phát hiện.
- **Kỹ Thuật Né Tránh Mới**: Ghi đè DLL trong bộ nhớ để loại bỏ quy trình agent của Sophos AV khỏi kernel, lạm dụng phần mềm AV để side-loading, và thử nghiệm nhiều kỹ thuật khác nhau để tìm ra phương pháp thực thi payload hiệu quả và khó bị phát hiện nhất.

Nguồn: https://thehackernews.com/2024/06/chinese-state-backed-cyber-espionage.html

Tin tức An toàn thông tin

"Chiến dịch tấn công APT: Chiến dịch tấn công mạng nhằm vào Đông Nam Á"

Qua quá trình phân tích chuyên sâu đã chỉ ra rằng các cụm hoạt động chồng chéo này có khả năng là một phần của một chiến dịch phối hợp do một tổ chức duy nhất chỉ đạo. Các cụm quan sát cho thấy hoạt động của một nhóm duy nhất với một loạt công cụ phong phú, cơ sở hạ tầng đa dạng và nhiều người vận hành.

Thông tin này xuất hiện cùng lúc với các cuộc tấn công của APT41 nhằm vào tổ chức ở Ý, sử dụng mã độc PlugX biến thể KEYPLUG. Được viết bằng C++ và hoạt động từ tháng 6/2021, KEYPLUG có phiên bản cho cả Windows và Linux, hỗ trợ nhiều giao thức mạng cho lưu lượng C2, là công cụ mạnh mẽ của APT41.

Trung tâm An ninh mạng Canada cũng đã cảnh báo về các cuộc tấn công gia tăng từ đối tượng tấn công mạng của Trung Quốc, nhằm vào chính phủ, cơ sở hạ tầng quan trọng và lĩnh vực nghiên cứu phát triển. Các cuộc tấn công này đặc biệt nguy hiểm với sự tinh vi và phạm vi mục tiêu rộng lớn, kèm theo việc sử dụng router văn phòng nhỏ và kỹ thuật living-off-the-land để tránh bị phát hiện.

Chiến dịch Crimson Palace là một ví dụ điển hình về sự phức tạp và kỹ thuật đa dạng của các cuộc tấn công mạng do chính phủ Trung Quốc tài trợ. Điều này đặc biệt đáng lo ngại khi các tổ chức chính phủ hàng đầu ở Đông Nam Á đang trở thành mục tiêu của chúng.

Một số IoC được ghi nhận:

89.44.197.74	scancenter.trendrealtime.com	185.195.237.123
195.123.247.50	172.67.130.71	45.90.58.103
185.195.237.121	104.21.3.57	185.82.217.164
195.123.245.79	associate.feedfoodconcerning.info	associate.freeonlinelearningtech.com
msudapis.info	154.39.137.29	147.139.47.141
185.167.116.30	associate.freeonlinelearning.com	91.220.202.143
139.162.18.97	message.ooguy.com	146.190.93.250
64.176.50.42	158.247.241.188	www.googlespeedtest33.com
139.180.217.105	45.130.229.181	185.201.8.187
198.13.47.158	0	0

Nguồn: https://thehackernews.com/2024/06/chinese-state-backed-cyber-espionage.html

NCSC VN
National Cyber Security Center

Tin tức An toàn thông tin

"Cảnh báo: TikTok khắc phục lỗ hổng zero-day sau chiến dịch chiếm dụng tài khoản người dùng"

Trong tuần vừa qua, đã có một số đối tượng tấn công chiếm dụng các tài khoản TikTok thuộc các cơ quan, tổ chức và của người nổi tiếng bằng cách khai thác một lỗ hổng zero-day tồn tại trong chức năng nhắn tin của nền tảng này.

Sau khi bị chiếm đoạt, các tài khoản của Sony, CNN,... đã bị TikTok tạm ngưng hoạt động để ngăn chặn việc các tài khoản này bị lợi dụng. Lỗ hổng an toàn thông tin này tồn tại trong tính năng nhắn tin của nền tảng TikTok. Đặc biệt, việc chiếm đoạt tài khoản xảy ra ngay khi người dùng mở một tin nhắn độc hại mà không cần phải tải xuống hoặc nhấp vào bất kỳ liên kết độc hại nào.

TikTok thông báo rằng họ đã nhận được cảnh báo về nguy cơ tấn công của lỗ hổng và đã thực hiện các biện pháp phòng ngừa để ngăn chặn việc tấn công, đồng thời, giảm thiểu nguy cơ tái diễn. Theo đánh giá ban đầu, chỉ một số nhỏ tài khoản TikTok bị ảnh hưởng bởi cuộc tấn công này. Hiện tại, thông tin chi tiết về lỗ hổng chưa được tiết lộ cho đến khi vấn đề được khắc phục một cách toàn diện.

Đây không phải lần đầu tiên Tiktok phát hiện lỗ hổng an toàn thông tin trong vài năm gần đây. Vào tháng 8 năm 2022, Microsoft đã ghi nhận lỗ hổng CVE-2022-28799 trên ứng dụng Android của TikTok, lỗ hổng này cho phép đối tượng tấn công chiếm quyền truy cập vào tài khoản người dùng chỉ với một lần chạm.

Trước đó, TikTok đã vá một lỗ hổng, cho phép đối tượng tấn công bỏ qua các biện pháp bảo vệ quyền riêng tư của người dùng để thu thập thông tin cá nhân như số điện thoại và ID người dùng. Hơn nữa, TikTok cũng đã phát hiện và vá một lỗ hổng khác, cho phép đối tượng tấn công chiếm quyền kiểm soát các tài khoản người dùng đã đăng ký thông qua các ứng dụng từ bên thứ ba. Chúng sử dụng các tài khoản này để đăng nội dung và lấy trộm thông tin cá nhân của người dùng.

Nguồn: https://www.bleepingcomputer.com/news/security/tiktok-fixes-zero-day-bug-used-to-hijack-high-profile-accounts/?&web_view=true

Nguy cơ tấn công mạng từ điểm yếu, lỗ hổng

Trong tuần, các tổ chức quốc tế đã công bố và cập nhật ít nhất **525** lỗ hổng, trong đó có 98 lỗ hổng mức Cao, 123 lỗ hổng mức Trung bình, 08 lỗ hổng mức Thấp và 296 lỗ hổng chưa đánh giá. Trong đó có ít nhất 108 lỗ hổng cho phép chèn và thực thi mã lệnh.

Ngoài ra, tuần hệ thống kỹ thuật của NCSC cũng đã ghi nhận TOP **10** lỗ hổng đáng chú ý, là những lỗ hổng có mức độ nghiêm trọng cao hoặc đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công.

Trong đó, đáng chú ý có **03** lỗ hổng ảnh hưởng các sản phẩm của Telerik, ngôn ngữ lập trình PHP và Oracle, cụ thể là như sau:

- **CVE-2024-4356 (Điểm CVSS: 9.8 – Nghiêm trọng):** Là lỗ hổng bỏ qua bước xác thực tồn tại trên Progress Telerik Report Server phiên bản cũ hơn 2024 Q1 (10.0.24.305) trên IIS, cho phép đối tượng tấn công có thể truy cập và thực hiện các hành vi trái phép trên chức năng hạn chế của máy chủ. Hiện lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.
- **CVE-2024-4577 (Điểm CVSS: 9.8 – Nghiêm trọng):** Là lỗ hổng tồn tại trong ngôn ngữ lập trình PHP trên Apache và PHP-CGI của Windows. Lỗ hổng xảy ra do Windows sử dụng hành vi "Best-Fit" để thay thế kí tự trong command line cung cấp tới hàm Win32 API. Đối tượng tấn công có thể khai thác lỗ hổng để truyền các tùy chỉnh độc hại tới binary PHP qua đó biết được mã nguồn, thực thi đoạn mã PHP tùy ý trên máy chủ. Hiện lỗ hổng đã có mã khai thác và đang bị khai thai thác trong thực tế.
- **CVE-2017-3506 (Điểm CVSS: 7.4 – Cao):** Lỗ hổng tồn tại trên thành phần Oracle WebLogic Server của Oracle Fusion Middleware cho phép đối tượng tấn công với khả năng truy cập vào hệ thống mạng của máy chủ qua giao thức HTTP, có thể truy cập và thực hiện các hành vi trái phép tới dữ liệu máy chủ. Hiện lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.

TOP 10 lỗ hổng đáng chú ý trong tuần

TT	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	CVE-2024-4358	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: Progress Telerik Report Server. - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực hiện các hành vi trái phép. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công.	https://nvd.nist.gov/vuln/detail/CVE-2024-4358
2	CVE-2024-4577	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: Ngôn ngữ lập trình PHP. - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực hiện các hành vi trái phép. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công.	https://nvd.nist.gov/vuln/detail/CVE-2024-4577
3	CVE-2017-3506	- Điểm CVSS: 7.4 (Cao) - Ảnh hưởng: Oracle Weblogic Server. - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực hiện các hành vi trái phép. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công.	https://nvd.nist.gov/vuln/detail/CVE-2017-3506
4	CVE-2024-24919	- Điểm CVSS: 8.6 (Cao) - Ảnh hưởng: Check Point Security Gateways - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực hiện các hành vi trái phép. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công.	https://nvd.nist.gov/vuln/detail/CVE-2024-24919
5	CVE-2024-27348	- Điểm CVSS: N/A - Ảnh hưởng: Apache. - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công.	https://nvd.nist.gov/vuln/detail/CVE-2024-27348

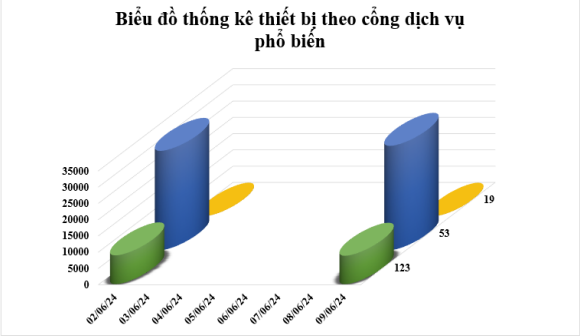
TOP 10 lỗ hổng đáng chú ý trong tuần

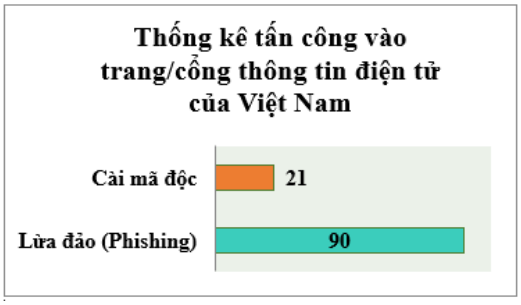
TT	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
6	CVE-2024-4367	- Điểm CVSS: 7.5 (Cao) - Ảnh hưởng: Mozilla Firefox, Mozilla Firefox ESR, Mozilla Thunderbird. - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực hiện script JavaScript tùy ý trên trình duyệt. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công.	https://nvd.nist.gov/vuln/detail/CVE-2024-4367
7	CVE-2024-3159	- Điểm CVSS: 8.8 (Cao) - Ảnh hưởng: Google Chrome. - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực hiện các hành vi trái phép. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công.	https://nvd.nist.gov/vuln/detail/CVE-2024-3159
8	CVE-2024-3400	- Điểm CVSS: 10 (Nghiêm trọng) - Ảnh hưởng: Palo Alto Networks PAN-OS - Mô tả: Lỗ hổng cho phép đối tượng thực thi mã từ xa. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong trong thực tế bởi các nhóm tấn công.	https://nvd.nist.gov/vuln/detail/CVE-2024-3400
9	CVE-2024-5274	- Điểm CVSS: 8.8 (Cao) - Ảnh hưởng: Google Chrome - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã tùy ý. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công.	https://nvd.nist.gov/vuln/detail/CVE-2024-5274
10	CVE-2024-29849	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: Veeam Backup Enterprise Manager - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực hiện các hành vi trái phép. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công.	https://nvd.nist.gov/vuln/detail/CVE-2024-29849

Thống kê nguy cơ, các cuộc tấn công mạng vào Việt Nam

Tấn công DRDoS

Tuần vừa qua tại Việt Nam, có rất nhiều máy chủ, thiết bị có thể trở thành nguồn phát tán tấn công DRDoS. Trong tuần có **40.819** (tăng so với tuần trước **39.409**) thiết bị có khả năng bị huy động và trở thành nguồn tấn công DRDoS. Các thiết bị này đang mở sử dụng các dịch vụ NTP (123), DNS (53), Chargen (19). Dưới đây là biểu đồ thống kê thiết bị theo cổng dịch vụ phổ biến trong tuần.



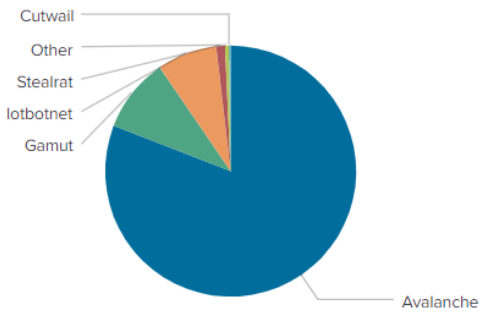


Tấn công Web

Trong tuần, có **111** trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 90 trường hợp tấn công lừa đảo (Phishing), 21 trường hợp tấn công cài cắm mã độc.

Botnet

Trên thế giới có nhiều địa chỉ IP/domain độc hại được các nhóm đối tượng tấn công sử dụng làm máy chủ C&C trong botnet. Những địa chỉ này cho phép nhóm đối tượng điều khiển thiết bị thuộc các mạng botnet để thực hiện các hành vi trái phép như triển khai tấn công DDoS, phát tán mã độc, gửi thư rác, truy cập và đánh cắp dữ liệu trên thiết bị. Trong tuần, ghi nhận **20** địa chỉ IP/domain thuộc botnet có ảnh hưởng tới người dùng Việt Nam.



Địa chỉ được sử dụng trong các mạng botnet

differentia.ru	restless.su
disorderstatus.ru	omfghellobrosjda38.org
atomictrivia.ru	andall.servicesql.info
amnsreiuojy.ru	griefcube.cc
xjpakmdcfuqe.biz	mcnodes.zapto.org
restlesz.su	sh5wyy1e.ru
hzmksreiuojy.ru	maxisurf.net
xjpakmdcfuqe.com	hfudrbdkr.org
xjpakmdcfuqe.ru	and3.dqnbnewproaaxies3.com
xjpakmdcfuqe.in	zzexidvyjlt.org

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có **388** phản ánh trường hợp lừa đảo do người dùng Internet Việt Nam phản ánh về Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC) qua hệ thống tại địa chỉ https://canhbao.khonggianmang.vn. Qua kiểm tra, phân tích có nhiều trường hợp lừa đảo giả mạo các tổ chức, doanh nghiệp, nhà cung cấp, dịch vụ lớn như: Các mạng xã hội, ngân hàng, thư điện tử,...

Dưới đây là một số trường hợp người dùng cần nâng cao cảnh giác.

STT	Website lừa đảo	Ghi chú
1	https://www[.]amatvip36sc[.]cc/	Website giả mạo sàn TMĐT Amazon
2	https://dienmayxanhctv24[.]com	Điện máy xanh
3	https://da2323[.]com	Website giả mạo sàn TMĐT Lazada
4	hdb[.]vntanghanmucvisadebit[.]com	Website giả mạo Ngân hàng TMCP Phát triển Thành phố Hồ Chí Minh
5	hdb[.]tang-han-muc-tin-dung-vn[.]com	Website giả mạo Ngân hàng TMCP Phát triển Thành phố Hồ Chí Minh
6	https://vnmcrd2s[.]online	Website giả mạo Ngân hàng TMCP Quân đội
7	vib-care[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
8	http://dich-vu-the-sat-vib[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
9	https://vib[.]chamsockhachhang-uudai-tructuyenthe[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
10	http://dich-vu-the-elite-vib[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
11	https://vib[.]chamsockhachhang-tructuyenuudaithe[.]online	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
12	dich-vu-the-vvip-vib[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
13	visa-vibbank[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
14	https://dich-vu-the-svip-vib[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
15	kh-vibquocte[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
16	https://sp75193p[.]com	Website giả mạo Website giả mạo sàn TMĐT Shopee
17	https://sp15569p[.]com/	Website giả mạo sàn TMĐT Shopee
18	https://fajiafu50[.]com	Website giả mạo sàn TMĐT Tiki
19	https://vntiki1[.]com	Website giả mạo sàn TMĐT Tiki
20	https://vntiki11[.]com/	Website giả mạo sàn TMĐT Tiki

NCSC VN
National Cyber Security Center

Khuyến nghị đối với các cơ quan, đơn vị

"NỖ LỰC ĐỂ KHÔNG GIAN MẠNG VIỆT NAM LUÔN AN TOÀN, LÀNH MẠNH"

1. Đối với các nguy cơ, cảnh báo đã được đề cập trong phần **Tin tức an toàn thông tin,** Quý đơn vị cần thường xuyên cập nhật thông tin (như các chiến dịch tấn công của các nhóm APT, thông tin IoC kèm theo từng chiến dịch, điểm yếu lỗ hổng đang bị lợi dụng để khai thác,…), rà soát trên các hệ thống thống thông tin để phát hiện và ngăn chặn, xử lý kịp thời.

***

2. Đối với các điểm yếu, lỗ hổng trong phần Lỗ hổng bảo mật, Quý đơn vị cần lưu ý theo dõi và cập nhật bản vá cho các lỗ hổng liên quan đến sản phẩm đang sử dụng. Ngoài ra, các đơn vị chủ động cập nhật các thông tin về các rủi ro an toàn thông tin mạng tại địa chỉ https://alert.khonggianmang.vn..

***

3. Đối với các nguy cơ về tấn công từ chối dịch vụ, tấn công web trong phần **Thống kê nguy cơ, các cuộc tấn công tại Việt Nam**, Quý đơn vị cần rà soát, hạn chế tối đa việc mở các cổng dịch vụ có thể bị lợi dụng để thực hiện tấn công từ chối dịch vụ; thường xuyên kiểm tra, rà soát máy chủ web để kịp thời phát hiện và xử lý nguy cơ tấn công. Bên cạnh đó, đối với các IP/tên miền được đề cập trong mục **Danh sách IP/tên miền độc hại có nhiều kết nối từ Việt Nam**, Quý đơn vị cần kiểm tra và xử lý các thiết bị trong toàn bộ hệ thống mạng nếu có dấu hiệu kết nối đến các tên miền độc hại mà Cục ATTT đã chia sẻ.

***

4. Đối với các website giả mạo thống kê tại mục **Tấn công lừa đảo người dùng Việt Nam**, Đề nghị các đơn vị, tổ chức, doanh nghiệp cần chủ động rà quét, phát hiện sớm các website lừa đảo giả mạo tổ chức của mình, cảnh báo sớm đến người dùng của nhằm ngăn chặn các hoạt động lừa đảo đến người dùng, đảm bảo an toàn thông tin cho người dùng, bảo vệ chính thương hiệu của tổ chức.

024.3209.1616
ncsc@ais.gov.vn
https://khonggianmang.vn/
https://www.facebook.com/govSOC
Tầng 16, số 115 Trần Duy Hưng, quận Cầu Giấy, Tp. Hà Nội